UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,760	03/04/2004	Masahiro Sueyoshi	249943US6	5272

22850 7590 12/15/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
KANE, CORDELIA P	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
12/15/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/791,760	SUEYOSHI ET AL.	
	Examiner	Art Unit	
	CORDELIA KANE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 12-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 3, 2008 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1 – 10, and 12 – 28 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1 – 10, 12 – 25, 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro, and further in view of Noguchi et al's US Publication 2002/0023216 A1.

5. Referring to claims 1, 27 and 28, Ishiguro teaches:

a. An authenticating means for authentication with a device to be authenticated on the basis of key data (page 3, paragraph 64).

b. A key generating means for generating said key data on the basis of the data received from said authenticating means and providing the same to said authenticating means (page 7, paragraph 105).

c. Wherein said authenticating means provides device identification data identifying the device to be authenticated and service identification data to said key generating means, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated, said key generating means generates said key data (page 7, paragraph 106).

6. Ishiguro does not explicitly disclose selecting a key generating algorithm corresponding to identification data from among a plurality of different algorithms and using the selected algorithm to generate the key. However, Noguchi discloses using ID2 to select the key generation algorithm from a plurality of algorithms, and then generating the key based on the ID2 (page 7, paragraph 77). Ishiguro and Noguchi are analogous art because they are from problem-solving area, secure communication. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Ishiguro and Noguchi before him or her, to modify the system of Ishiguro to include the selecting of the key generation algorithm of Noguchi. The suggestion/motivation for doing so would have been so that the source and destination

of a public key for verification of data integrity do not necessarily match the source and destination of a main transmission (i.e. cipher transmission using a symmetric key) after the verification of data integrity, so that the inverse relation may be allowed (page 5, paragraph 57).

7. Referring to claim 2, Ishiguro teaches the key generating means generates said key data unique to the device on the basis of the data received from the authenticating means (page 7, paragraph 106).

8. Referring to claim 3, Ishiguro teaches the key generating means is provided with a function module having a first input parameter and a second input parameter and generating said key data by using only said first data entered for said first input parameter and said authenticating means enters said first data for said first input parameter of said function module of said key generating means and enters said second data for said second parameter (page 7, paragraph 106).

9. Referring to claim 4, Ishiguro teaches that the authenticating means provides identification data relating to processing to be performed after said authentication to said key generating means (page 7, paragraph 5).

10. Referring to claims 5 and 6, Ishiguro teaches that the authentication module provides a function module for performing processing for providing unique data to said device to be authenticated received from said device to be authenticated, and said key generating means calls up said function module of said authenticating means and further uses said unique data received from said function module to generate said key data (page 6, paragraph 98).

11. Referring to claim 7, Ishiguro teaches the authenticating means providing the unique data from a storage means shared between said authenticating means and generating means (Figure 8).

12. Referring to claims 8 and 9, Ishiguro teaches a key holding means for reading out master key data and holding master key data, and said key generating means calls up the key holding means and uses the master key obtained to generate said key data (page 9, paragraph 128).

13. Referring to claim 10, Ishiguro teaches that the key holding program is updated independently from programs for realizing said authenticating and key generating means (page 9, paragraph 128).

14. Referring to claim 12, Ishiguro teaches performing authentication with said device to be authenticated on the basis of key data and when recognizing mutual legitimacy with said device to be authenticated performing processing corresponding to said key data in cooperation with said device to be authenticated (page 1, paragraph 5).

15. Referring to claim 13, Ishiguro teaches performing first authentication using fixed key data (page 4, paragraph 73) and then performs second authentication using individual key data generated (page 4, paragraph 75).

16. Referring to claim 14, Ishiguro teaches confirming legitimacy of the device to be authenticated before proceeding with second authentication (page 4, paragraph 73).

17. Referring to claim 15, Ishiguro teaches generating the individual key data using data unique to the device to be authenticated and the original key data (page 4, paragraphs 73-75).

18. Referring to claim 16, Ishiguro teaches holding identification data of processing to be performed with said device to be authenticated linked with the original key data and provides said key generating means with said original key data and generating the key based on the original key data (page 4, paragraph 75).

19. Referring to claims 17 and 23, Ishiguro teaches:

d. Receiving from said authenticating means device identification data identifying the device to be authenticated and service identification data at said key generating means, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated (page 7, paragraph 106).

e. Generating key data with said key generating means by using only one of said first service identification data or said second service identification data (page 7, paragraph 105).

f. Providing the key data to said authenticating means (page 7, paragraph 105).

g. Authenticating with said authenticating means the device to be authenticated on the basis of said key data received at said providing (page 3, paragraph 64).

20. Ishiguro does not explicitly disclose selecting a key generating algorithm corresponding to identification data from among a plurality of different algorithms and

using the selected algorithm to generate the key. However, Noguchi discloses using ID2 to select the key generation algorithm from a plurality of algorithms, and then generating the key based on the ID2 (page 7, paragraph 77). Ishiguro and Noguchi are analogous art because they are from problem-solving area, secure communication. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Ishiguro and Noguchi before him or her, to modify the system of Ishiguro to include the selecting of the key generation algorithm of Noguchi. The suggestion/motivation for doing so would have been so that the source and destination of a public key for verification of data integrity do not necessarily match the source and destination of a main transmission (i.e. cipher transmission using a symmetric key) after the verification of data integrity, so that the inverse relation may be allowed (page 5, paragraph 57).

21. Referring to claims 18 and 24, Ishiguro teaches generating said key data unique to said device to be authenticated on the basis of data received from said authenticating means (page 7, paragraph 106).

22. Referring to claims 19 and 25, Ishiguro teaches the key generating means is provided with a function module having a first input parameter and a second input parameter and generating said key data by using only said first data entered for said first input parameter and said authenticating means enters said first data for said first input parameter of said function module of said key generating means and enters said second data for said second parameter (page 7, paragraph 106).

23. Referring to claim 20, Ishiguro teaches said key generating means calls up said function module of said authenticating means and further uses said unique data received from said function module to generate said key data (page 6, paragraph 98).

24. Referring to claim 21, Ishiguro teaches said key generating means calls up the key holding means and uses the master key obtained to generate said key data (page 9, paragraph 128).

25. Referring to claim 22, Ishiguro teaches updating a key holding program for realizing said key holding means independently from a program for realizing said authenticating means and said key generating means (page 9, paragraph 128).

26. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro in view of Noguchi as applied above, and further in view of Akkermans et al's US Publication 2006/0104449 A1. Ishiguro in view of Noguchi discloses all the limitations of the parent claim. Ishiguro in view of Noguchi does not explicitly disclose having access rights different from said authentication program. However, Akkermans discloses that a DVD has a restriction to permit playback only once or N time (page 5, paragraph 57). Ishiguro in view of Noguchi and Akkermans are analogous art because they are from the same field of endeavor, DVDs. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Ishiguro in view of Noguchi and Akkermans before him or her, to modify the DVD of Ishiguro in view of Noguchi to include the access rights of Akkermans. The suggestion/motivation for doing

so would have been to limit the amount of times a DVD is played (page 5, paragraph 57).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA KANE whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. K./
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432